PCT

WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 :
H04L 9/08

A1

(11) Internationale Veröffentlichungsnummer: WO 97/47109

(43) Internationales Veröffentlichungsdatum: 11. Dezember 1997 (11.12.97)

(21) Internationales Aktenzeichen: PCT/DE97/01002

(22) Internationales Anmeldedatum: 16. Mai 1997 (16.05.97)

(30) Prioritätsdaten:
196 22 631.7 5. Juni 1996 (05.06.96) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, D-80333 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: EUCHNER, Martin [DE/DE]; Lorenzstrasse 2, D-81737 München (DE). KESSLER, Volker [DE/DE]; Pfarrer-Schmitter-Strasse 1, D-85256 Vierkirchen (DE).

(81) Bestimmungsstaaten: BR, CA, CN, JP, KR, MX, RU, UA, US, europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist. Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: PROCESS FOR CRYPTOGRAPHIC CODE MANAGEMENT BETWEEN A FIRST COMPUTER UNIT AND A SECOND COMPUTER UNIT

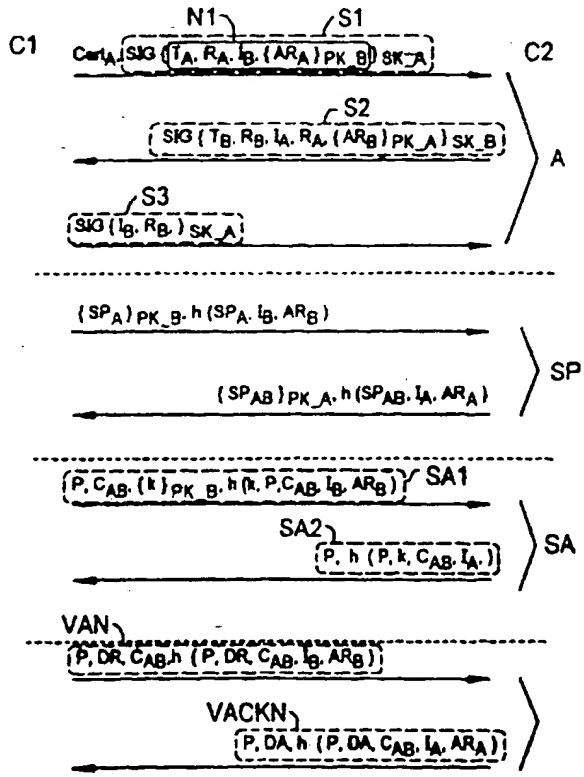
(54) Bezeichnung: VERFAHREN ZUM KRYPTOGRAPHISCHEN SCHLÜSSELMANAGEMENT ZWISCHEN EINER ERSTEN COMPUTEREINHEIT UND EINER ZWEITEN COMPUTEREINHEIT

(57) Abstract

The invention relates to a process which is divided into individual modular phases. During authentication of the first computer unit (C1) and the second computer unit (C2), authentication references (AR_A, AR_B) are exchanged and are used in further cryptographic phases (SP, SA) thereby eliminating, also as a result of the modular structure, the need for new authentication which is actually required in each case in the other cryptographic phases (SP, SA), said authentication being also no longer performed.

(57) Zusammenfassung

Das Verfahren ist in einzelne modulare Phasen aufgeteilt. Während einer Authentifikation der ersten Computereinheit (C1) und der zweiten Computereinheit (C2) werden Authentifikationsreferenzen (AR_A, AR_B) ausgetauscht, die in weiteren kryptographischen Phasen (SP, SA) verwendet werden. Dadurch und durch den modularen Aufbau ist eine in den weiteren kryptographischen Phasen (SP, SA) eigentlich benötigte jeweils neue Authentifikation nicht mehr erforderlich und wird auch nicht mehr durchgeführt.



LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss PCT veröffentlichen.

AL	Albanien
AM	Armenien
AT	Österreich
AU	Australien
AZ	Aserbaidschan
BA	Bosnien-Herzegowina
BB	Barbados
BE	Belgien
BF	Burkina Faso
BG	Bulgarien
BJ	Benin
BR	Brasilien
BY	Belarus
CA	Kanada
CF	Zentralafrikanische Republik
CG	Kongo
CH	Schweiz
CI	Côte d'Ivoire
CM	Kamerun
CN	China
CU	Kuba
CZ	Tschechische Republik
DE	Deutschland
DK	Dänemark
EE	Estland
ES	Spanien
FI	Finnland
FR	Frankreich
GA	Gabun
GB	Vereinigtes Königreich
GE	Georgien
GH	Ghana
GN	Guinea
GR	Griechenland
HU	Ungarn
IE	Irland
IL	Israel
IS	Island
IT	Italien
JP	Japan
KE	Kenia
KG	Kirgisistan
KP	Demokratische Volksrepublik Korea
KR	Republik Korea
KZ	Kasachstan
LC	St. Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Litauen
LU	Luxemburg
LV	Lettland
MC	Monaco
MD	Republik Moldau
MG	Madagaskar
MK	Die ehemalige jugoslawische Republik Mazedonien
ML	Mali
MN	Mongolei
MR	Mauretanien
MW	Malawi
MX	Mexiko
NE	Niger
NL	Niederlande
NO	Norwegen
NZ	Neuseeland
PL	Polen
PT	Portugal
RO	Rumänien
RU	Russische Föderation
SD	Sudan
SE	Schweden
SG	Singapur
SI	Slowenien
SK	Slowakei
SN	Senegal
SZ	Swasiland
TD	Tschad
TG	Togo
TJ	Tadschikistan
TM	Turkmenistan
TR	Türkei
TT	Trinidad und Tobago
UA	Ukraine
UG	Uganda
US	Vereinigte Staaten von Amerika
UZ	Usbekistan
VN	Vietnam
YU	Jugoslawien
ZW	Zimbabwe

Beschreibung

Verfahren zum kryptographischen Schlüsselmanagement zwischen einer ersten Computereinheit und einer zweiten Computereinheit

Bei einer Kommunikation zwischen Kommunikationsteilnehmern ist es in vielen technischen Bereichen notwendig, die Kommunikation der Teilnehmer mittels kryptographischer Verfahren gegen jeglichen Mißbrauch abzusichern. Dabei ist der Aufwand, der für eine kryptographische Absicherung der gesamten Kommunikation erforderlich ist, abhängig von der jeweiligen Anwendung. So ist es beispielsweise in Privatgesprächen unter Umständen nicht von sehr großer Bedeutung, daß alle kryptographisch möglichen Sicherheitsmaßnahmen zur Absicherung der Kommunikation getroffen werden. Bei Kommunikation mit sehr vertraulichem Inhalt ist jedoch beispielsweise eine sehr strikte Absicherung der Kommunikation von erheblicher Bedeutung.

Die Auswahl von für die Absicherung der Kommunikation verwendeten Sicherheitsdiensten, Sicherheitsmechanismen, Sicherheitsalgorithmen und Sicherheitsparametern wird als Sicherheitspolitik, die während der Kommunikation zwischen Kommunikationspartnern eingehalten wird, bezeichnet.

Da jedoch das Sicherheitsbedürfnis und damit verbunden die Sicherheitspolitik von Kommunikationssitzung zu Kommunikationssitzung und von Anwendung zu Anwendung unterschiedlich ist und da die Kommunikationsteilnehmer tatsächlich nicht über alle kryptographischen Verfahren verfügen, kann es bei häufig wechselnden Kommunikationspartnern zu schwerwiegenden Diskrepanzen in der erforderlichen bzw. möglichen Sicherheitspolitik kommen, die von der jeweiligen Computereinheit des Kommunikationspartners unterstützt wird und somit gewährleistet werden kann.

Es ist erforderlich, daß in jeder Kommunikationssitzung innerhalb einer Gruppe, die an einer Kommunikationssitzung teilnimmt, eine einheitliche Sicherheitspolitik für die jeweilige Kommunikation festgelegt wird.

Bei einer Vielzahl unterschiedlicher Applikationsprotokolle, welche beispielsweise in dem Dokument [1] beschrieben sind , z. B. CMAP, CDAP, etc., tritt das Problem auf, daß verschiedene Applikationsprotokolle gleicher oder verschiedener Computereinheiten eine unterschiedliche Sicherheitspolitik benötigen. Es werden eventuell auch eigene, für das jeweilige Applikationsprotokoll spezifische kryptographische Schlüssel für eine logische Verbindung des jeweiligen Applikationsprotokolls zwischen zwei Computereinheiten benötigt. Da verschiedene Applikationsprotokolle auf einer Computereinheit implementiert sein können, müssen unter Umständen mehrere kryptographische Schlüssel zwischen zwei Computereinheiten ausgetauscht werden. Auch kann es aus diesem Grund nötig sein, mehrere verschiedene Sicherheitspolitiken zwischen zwei Computereinheiten auszuhandeln.

Ein sicherer Schlüsselaustausch oder eine vertrauenswürdige Aushandlung einer Sicherheitspolitik basiert auf einer gegenseitigen Authentifikation der in die Aushandlung bzw. in den Schlüsselaustausch involvierten Computereinheiten vor dem eigentlichen Schlüsselaustausch bzw. der Aushandlung der Sicherheitspolitik.

Es wird üblicherweise vor jeder Aushandlung einer Sicherheitspolitik bzw. vor jedem Schlüsselaustausch eine Authentifikationsphase durchgeführt, in der die Computereinheiten sich gegenseitig authentifizieren.

Dies führt bei einer Vielzahl von Aushandlungen einer Sicherheitspolitik oder Schlüsselaustauschvorgängen zu einer Vielzahl von durchgeführten Authentifikationen, die einen erhöh-

ten Kommunikationsaufwand und erhöhten Bedarf an Rechenkapazität bedeuten.

Dieses Problem wird noch verschärft, wenn nicht nur zwei Computereinheiten miteinander kommunizieren, sondern wenn mehrere Computereinheiten vorgesehen sind, die verschiedenen Sicherheitsdomänen zugeordnet werden. Unter einer Sicherheitsdomäne ist in diesem Zusammenhang eine Menge von Computereinheiten zu verstehen, die eine gemeinsame Sicherheitspolitik verfolgen.

In diesem Fall wird üblicherweise die Authentifikation auf Basis der Sicherheitsdomänen durchgeführt.

Eine Übersicht über allgemein verwendbare kryptographische Verfahren, die in dem Verfahren eingesetzt werden können, ist beispielsweise in dem Dokument [2] zu finden.

Es ist bekannt, zwischen zwei Kommunikationspartnern eine Sicherheitspolitik auszuhandeln, wobei sich jedoch die in diesem Dokument beschriebene Aushandlung nur auf wenige, zuvor festgelegte Parameter beschränkt ist [3].

Der Erfindung liegt das Problem zugrunde, ein Verfahren zum Schlüsselmanagement zwischen zwei Computereinheiten anzugeben, bei dem der benötigte Kommunikationsaufwand und die zur Durchführung des Verfahrens benötigte Rechenkapazität geringer ist als bei bekannten Verfahren.

Das Problem wird durch das Verfahren gemäß Patentanspruch 1 gelöst.

Bei dem Verfahren wird eine Authentifikation zwischen zwei Computereinheiten durchgeführt, in deren Rahmen Authentifikationsreferenzen zwischen den Computereinheiten ausgetauscht werden. Mit den Authentifikationsreferenzen wird eine geheime Information zwischen den Computereinheiten ausgetauscht, an-

hand derer eine Authentifikation der Computereinheiten möglich ist. Eine anschließende Aushandlung einer Sicherheitspolitik und/oder ein anschließender Schlüsselaustausch zwischen den Computereinheiten erfolgt unter Verwendung der Authentifikationsreferenzen.

Durch dieses Verfahren ist es möglich, explizite Authentifikationsphasen zwischen den Computereinheiten für jeden neuen Schlüsselaustausch und/oder für jede neue Aushandlung einer Sicherheitspolitik zu vermeiden. Dies bedeutet beispielsweise bei einer Vielzahl von eingesetzten Applikationsprotokollen eine erhebliche Reduktion benötigter Authentifikationsphasen, da die Authentifikation nur einmal zwischen den Computereinheiten durchgeführt werden muß und für alle weiteren Schritte die Authentifikation der Computereinheiten implizit anhand der mit übertragenen Authentifikationsreferenzen erfolgt.

Damit wird der für ein Schlüsselmanagement benötigte Kommunikationsaufwand zwischen den Computereinheiten sowie der benötigte Rechenzeitbedarf erheblich reduziert.

Vorteilhafte Weiterbildungen der Erfindung ergeben sich aus den abhängigen Ansprüchen.

Bei Gruppierung einer Vielzahl von Computereinheiten in Sicherheitsdomänen und einer Authentifikation der Computereinheiten auf Basis der Sicherheitsdomäne, der die jeweilige Computereinheit zugeordnet ist, wird eine weitere Einsparung benötigten Kommunikationsaufwands und benötigter Rechenkapazität erreicht. Dies wird durch den modularen Aufbau des Verfahrens erreicht, da nur für jeweils eine Computereinheit einer Sicherheitsdomäne eine explizite Authentifikationsphase durchgeführt werden muß. Werden Aushandlungen einer weiteren Sicherheitspolitik und/oder ein weiterer Schlüsselaustausch zwischen weiteren Computereinheiten der entsprechenden Sicherheitsdomänen, für die schon eine gegenseitige Authentifikation erfolgte, können die ausgetauschten Authentifikations-

referenzen bei der weiteren Aushandlung und/oder dem weiteren Schlüsselaustausch implizit zur Authentifikation der weiteren Computereinheiten eingesetzt werden.

Ferner ist es in einer Weiterbildung des Verfahrens vorteilhaft, Hash-Funktionen zu verwenden, die auf symmetrischen Kryptoalgorithmen basieren, da eine Bildung von Hash-Werten unter Verwendung von solchen Hash-Funktionen sehr schnell durchgeführt werden kann. Damit wird die Durchführung des Verfahrens erheblich beschleunigt.

Durch Verwendung Digitaler Signaturen in dem Verfahren wird eine vertrauenswürdige, nicht abstreitbare Durchführung des Verfahrens möglich.

Weiterhin ist es vorteilhaft, eine Verbindungsabbauphase (Disconnect) durchzuführen, in deren Rahmen geteilte Geheimnisse, beispielsweise der ausgetauschte Schlüssel oder die Authentifikationreferenzen gelöscht werden. Damit wird die Sicherheit des Verfahrens weiter erhöht, da keine ausgetauschten geheimen Informationen für andere Computereinheiten zum eventuellen späteren Mißbrauch zur Verfügung stehen. Die Verbindungsabbauphase dient weiterhin zur Synchronisation der bei der Kommunikation beteiligten Computereinheiten.

In einer Weiterbildung des Verfahrens ist es vorteilhaft, die geheimen Informationen sukzessive zu löschen, so daß eine hierarchische Wiederverwendung geheimer, zuvor ausgetauschter Information z. B. bei weiterem Austausch von Schlüsseln möglich ist. Dies bedeutet beispielsweise, daß zu Beginn der Verbindungsabbauphase der für die logische Verbindung ausgetauschte Sitzungsschlüssel gelöscht wird, die zwischen den Applikationsprotokollen ausgehandelte Sicherheitspolitik noch gespeichert bleibt. Bei einer anschließenden neuen logischen Verbindung zwischen den Applikationsprotokollen der Computereinheiten ist es dann lediglich erforderlich, einen neuen Schlüssel zwischen den Computereinheiten auszutauschen. Die

zuvor ausgetauschen geheimen Informationen, beispielsweise die Authentifikationsreferenzen oder die ausgehandelte Sicherheitspolitik kann weiter auch bei der neuen logischen Verbindung wieder verwendet werden.

In den Figuren ist ein Ausführungsbeispiel der Erfindung dargestellt, welches im weiteren näher erläutert wird.

Es zeigen

Fig. 1 ein Ablaufdiagramm, in dem die einzelnen Verfahrensschritte des Verfahrens dargestellt sind.

Fig. 2 eine Skizze eines Nachrichtenformats, in dem die bei dem Verfahren ausgetauschten Nachrichten vorteilhaft übertragen werden können.

Im Rahmen dieser Erfindung ist der Begriff des kryptographische Verfahrens in einer Weise zu verstehen, daß sowohl alle kryptographische Verfahren als auch die nichtkryptographische Verfahren zur Integritätsprüfung des Datenpakets DP, beispielsweise der Cyclic-Redundancy Check (CRC) mit dem Begriff kryptographisches Verfahren bezeichnet werden.

In Figur 1 ist ein Beispiel des Verfahrens dargestellt, anhand dessen die Erfindung dargestellt wird. Wie im weiteren erläutert wird, ist dieses Auführungsbeispiel keinesfalls als ausschließliche Realisierungsmöglichkeit der Erfindung zu verstehen. Varianten des Ausführungsbeispiels in den einzelnen Verfahrensschritten sind für den Fachmann bekannt und werden im Rahmen der weiteren Beschreibung erläutert.

Zu Beginn des Verfahrens wird zwischen einer ersten Computereinheit C1 und einer zweiten Computereinheit C2 eine Authentifikation durchgeführt. Die Authentifikation erfolgt in einer Authentifikationsphase A.

Die Authentifikation kann beispielsweise nach dem in dem X.509-Standard beschriebenen Verfahren zur starken Authentifikation erfolgen. Dies Authentifikation wird dabei beispielsweise auf folgende Weise durchgeführt.

Von der ersten Computereinheit C1 wird ein erstes Zertifikat $Cert_A$, welches einen vertrauenswürdigen, von einer vertrauenswürdigen dritten Instanz, der Zertifizierungseinheit zertifizierten, öffentlichen Schlüssel der ersten Computereinheit C1 enthält, zu einer zweiten Copmutereinheit C2 übertragen.

Ferner wird von der ersten Computereinheit C1 zusätzlich zu dem ersten Zertifikat $Cert_A$ eine erste Signaturnachricht S1 gebildet, die durch eine digitale Unterschrift über eine erste Nachricht N1 mit einem geheimen Schlüssel SK_A der ersten Computereinheit C1 gebildet wird.

Die erste Nachricht N1 enthält beispielsweise einen ersten Zeitstempel T_A, eine erste Zufallszahl R_A, die im Rahmen dieses Verfahrens eindeutig ist, eine Identitätsangabe I_B der zweiten Computereinheit C2, bei Verwendung des X.509-Authentifikationsmechanismus beispielsweise die eindeutige Identitätsangabe der zweiten Computereinheit C2, bei einer im weiteren beschriebenen Aushandlung einer zu verwendenden Sicherheispolitik, die sich über eine ganze Sicherheitsdomäne erstreckt, eine Domänenangabe SDID, der die zweite Computereinheit C1 zugeordnet wird, sowie eine mit einem öffentlichen Schlüssel PK_B der zweiten Computereinheit C2 verschlüsselte Authentifikationsreferenz AR_A der ersten Computereinheit C1, die einem Pseudoschlüssel der ersten Computereinheit C1 entspricht

Das erste Zertifikat $Cert_A$ sowie die erste Signaturnachricht S1 wird an die zweite Computereinheit C2 übertragen.

Nach Auswertung (Verifizierung) der ersten Signaturnachricht S1, welche zur Abwehr von kryptographischen Angriffen unterschiedlicher Art dient, wird in der zweiten Computereinheit C2 eine zweite Signaturnachricht S2 gebildet und an die erste Computereinheit C1 übertragen.

Die zweite Signaturnachricht S2 enthält beispielsweise folgende Komponenten:

- einen zweiten Zeitstempel T_B,
- eine zweite, eindeutige Zufallszahl R_B,
- eine Identitätsangabe I_A der ersten Computereinheit C1,
- die erste Zufallszahl R_A,
- eine mit einem öffentlichen Schlüssel PK_A der ersten Computereinheit C1 verschlüsselte Authentifikationsreferenz AR_B der zweiten Computereinheit C2.

Die oben beschriebenen Komponenten bilden eine zweite Nachricht N2, die durch Bildung einer digitalen Unterschrift unter Verwendung eines geheimen Schlüssels SK_B der zweiten Computereinheit C2 bestimmt wird.

Die geheimen Pseudoschlüssel in Funktion der Authentifikationsreferenz AR_A der ersten Computereinheit C1 und der Authentifikationsreferenz AR_B der zweiten Computereinheit C2 dienen im weiteren Protokollablauf dazu, nachfolgende Protokollphasen und Protokollnachrichten kryptographisch an die Authentifikationsphase zu koppeln. Bei Verwendung des X.509-Standards kann die Authentifikationsreferenz AR_A der ersten Computereinheit C1 in einem Feld übertragen werden, das für einen „geheimen Bit-String" vorgesehen ist.

Nach Empfang und Auswertung, d. h. Verifizierung der zweiten Signaturnachricht S2 in der ersten Computereinheit C1 wird von der ersten Computereinheit C1 eine dritte Signaturnachricht S3 gebildet und an die zweite Computereinheit C2 übertragen.

Die dritte Signaturnachricht S3 wird gebildet unter Verwendung des geheimen Schlüssels SK_A der ersten Computereinheit C1, mit dem eine dritte Nachricht N3 verschlüsselt wird. Die dritte Nachricht N3 enthält mindestens die Identitätsangabe I_B der zweiten Computereinheit C2 sowie die zweite Zufallszahl R_B.

Die Authentifikation kann jedoch durch jede andere Authentifikation zwischen der ersten Computereinheit C1 und der zweiten Computereinheit C2 erfolgen, beispielsweise unter Verwendung des Prinzips des exponentiellen Schlüsselaustauschs, z. B. unter Verwendung des sog. Diffie-Hellmann-Verfahrens. Bei Verwendung des Diffie-Hellmann-Schlüsselaustauschs wird der ausgetauschte Schlüssel direkt als die im weiteren Verfahren verwendete Authentifikationsreferenzen AR_A, AR_B verwendet.

In der Authentifikationsphase A ist es lediglich erforderlich, daß zwischen der ersten Computereinheit C1 und der zweiten Computereinheit C2 die Authentifikationsreferenzen AR_A, AR_B in vertrauenswürdiger Weise ausgetauscht werden. Dies bedeutet, daß es nur erforderlich ist, daß in den beiden Computereinheiten C1, C2 eine für die jeweilige Computereinheit C1, C2 charakteristische geheime Information in der jeweiligen anderen Computereinheit C1, C2 nach der Authentifikationsphase A vorliegt.

Nach erfolgter Authentifikation wird zwischen der ersten Computereinheit C1 und der zweiten Computereinheit C2 eine in der weiteren Kommunikationsphase eingesetzte Sicherheitspolitik ausgehandelt und/oder es wird ein kryptographische Schlüssel ausgetauscht.

Im weiteren werden sowohl eine Aushandlungsphase SP der Sicherheitspolitik als auch eine Schlüselaustauschphase SA detailliert erläutert. Es ist jedoch in Varianten des Verfahren vorgesehen, nur die Aushandlungsphase SP der Sicherheitspolitik oder die Schlüselaustauschphase SA durchzuführen. Die

gemeinsame Darstellung beider Phasen SP, SA in dem Ausführungsbeispiel dient lediglich der deutlicheren Darstellung der Erfindung.

Die Aushandlungsphase SP der Sicherheitspolitik kann beispielsweise durch folgende Verfahrensschritte charakterisiert sein.

Mit diesem modular aufgebauten Protokoll wird eine gegenseitige Authentifikation der ersten Computereinheit C1 und der zweiten Computereinheit C2 für weitere Aushandlungen der Sicherheitspolitik zwischen der ersten Computereinheit C1 und der zweiten Computereinheit C2 möglich, ohne daß die Authentifikationsphase A erneut durchführen zu müssen. Dies wird durch Verwendung der Authentifikationsreferenzen AR_A, AR_B in der Aushandlungsphase SP der Sicherheitspolitik zur impliziten Authentifikation der Computereinheiten C1, C2 möglich.

Die Sicherheitspolitik kann sich in einer Weiterbildung beispielsweise über ganze Sicherheitsdomänen S1, S2 erstrecken, womit eine Gruppe von Rechnern bezeichnet wird, die sich einer gemeinsamen Sicherheitspolitik unterordnen.

Die Sicherheitspolitik kann sich jedoch auch nur auf die aktuell aufzubauende Verbindung zwischen der ersten Computereinheit C1 und der zweiten Computereinheit C2 erstrecken.

Es wird ein Sicherheitspolitikvorschlag SP_A, der die zu verwendende Sicherheitspolitik, die von der ersten Computereinheit C1 vorgeschlagen wird, enthält, in der ersten Computereinheit C1 gebildet.

Der Sicherheitspolitikvorschlag SP_A wird mit dem öffentlichen Schlüssel PK_B der zweiten Computereinheit C2 verschlüsselt, wodurch der sensitive Sicherheitspolitikvorschlag SP_A vor einem unbefugten Abhören geschützt wird.

Ferner wird mindestens auf den Sicherheitspolitikvorschlag SP_A, die Identitätsangabe I_B der zweiten Computereinheit C2 sowie die Authentifikationsreferenz AR_B der zweiten Computereinheit C2 eine Hash-Funktion h(.) angewendet wird, mit der ein erster Hash-Wert $h(SP_A, I_B, AR_B)$ gebildet wird.

Mit dem ersten Hash-Wert $h(SP_A, I_B, AR_B)$ wird die Authentizität der ersten Computereinheit C1 sowie des Sicherheitspolitikvorschlags SP_A gewährleistet für die zweite Computereinheit C2.

Es ist an dieser Stelle möglich ist, eine asymmetrische digitale Unterschrift zu verwenden, wodurch eine Nichtabstreitbarkeit der jeweils digital signierten Nachricht erreicht wird.

Die Bildung eines Hash-Wertes auf Basis symmetrischer Kryptoverfahren weist den Vorteil auf, daß die Ermittlung des Hash-Wertes mittels symmetrischer Kryptoverfahren erheblich schneller durchgeführt werden kann als die Bildung einer digitalen Unterschrift.

Es können beliebige Hash-Funktionen im Rahmen dieses Verfahrens eingesetzt werden, beispielsweise das MD4-Verfahren, das MD5-Verfahren, oder der Hash-Algorithmus ISO10118. Das Hash-Verfahren ISO10118 ist besonders vorteilhaft einsetzbar für den Fall, wenn eine Hardwareimplimentierung des symmetrischen sog. DES-Verschlüsselungsverfahrens (Data Encryption Standard) vorhanden ist.

Der verschlüsselte Sicherheitspolitikvorschlag SP_A sowie der erste Wert $h(SP_A, I_B, AR_B)$ werden zu der zweiten Computereinheit C2 übertragen und dort verifiziert.

Als Antwort wird eine Sicherheitspolitikbestätigung SP_{AB} zu der ersten Computereinheit C1 übertragen, die mit dem öffentlichen Schlüssel PK_A der ersten Computereinheit C1 ver-

schlüsselt wird. Ferner wird ein zweiter Hash-Wert $h(SP_{AB}, I_A, AR_A)$ in der zweiten Computereinheit C2 gebildet und zu der ersten Computereinheit C1 übertragen, wobei der zweite Hash-Wert $h(SP_{AB}, I_A, AR_A)$ mindestens über die Sicherheitspolitikbestätigung SP_{AB}, die Identitätsangabe I_A der ersten Computereinheit C1 sowie die Authentifikationsreferenz AR_A der ersten Computereinheit C1 gebildet wird.

Die Sicherheitspolitikbestätigung SP_{AB} enthält beispielsweise entweder eine Bestätigung der Akzeptanz des von der ersten Computereinheit C1 gesendeten Sicherheitspolitikvorschlags SP_A, oder aber einen eigenen, von der zweiten Computereinheit C2 gebildeten Sicherheitspolitikvorschlag. Weicht der von der zweiten Computereinheit C2 gebildete Sicherheitspolitikvorschlag von dem Sicherheitspolitikvorschlag SP_A der ersten Computereinheit C1 ab, so muß auf entsprechende Weise die erste Computereinheit C1 den weiteren Sicherheitspolitikvorschlag verarbeiten, verifizieren, überprüfen und eine weitere Sicherheitspolitikbestätigung zu der zweiten Computereinheit C2 senden.

Die Inhalte der Nachrichten sind entsprechend dem oben beschriebenen Verfahren. Die Aushandlungsphase SP der Sicherheitspolitik kann iterativ solange weitergeführt werden, bis sich die erste Computereinheit C1 und die zweite Computereinheit C2 auf eine einheitliche, von beiden Computereinheiten C1, C2 unterstützte Sicherheitspolitik „geeinigt" haben.

Die Schlüselaustauschphase SA kann beispielsweise durch folgende Verfahrensschritte realisiert werden.

Von der ersten Computereinheit C1 wird eine erste Schlüsselaustauschnachricht SA1 zu der zweiten Computereinheit C2 übertragen.

Die erste Schlüsselaustauschnachricht SA1 enthält beispielsweise folgende Komponenten:

- eine Angabe P einer zu verwendenden Verbindung, mit der eine von mehreren verschiedenen gleichzeitig aktiven Verbindungen repräsentiert wird,
- einen Zählwert C_{AB} der ersten Computereinheit C1 für die Schlüsselverteilung und/oder eine Verbindungsabbruchsnachricht,
- einen mit dem öffentlichen Schlüssel PK_B der zweiten Computereinheit C2 verschlüsselten, im weiteren Verfahren zu verwendenden Sitzungsschlüssel k, wobei der Sitzungsschlüssel k vorteilhafterweise ein symmetrischer Sitzungsschlüssel ist, der im Rahmen der Verbindung P eingesetzt wird,
- ein dritter Hash-Wert $h(k, P, C_{AB}, I_B, AR_B)$, der gebildet wird mindestens über den Sitzungsschlüssel k, die Verbindung P, den Zählwert C_{AB}, die Identitätsangabe I_B der zweiten Computereinheit C2 sowie die Authentifikationsreferenz AR_B der zweiten Computereinheit C2.

Es ist in einer Weiterbildung des Verfahrens ebenfalls vorgesehen, daß der Sitzungsschlüssel k ein asymmetrisches Schlüsselpaar ist.

Der Zählwert C_{AB} zwischen der ersten Computereinheit C1 und der zweiten Computereinheit C2 dient dazu, zwischen verschiedenen Protokolldurchläufen für die gleiche Verbindung P zwischen der ersten Computereinheit C1 und der zweiten Computereinheit C2 zu unterscheiden. Indem der jeweils empfangene Zählwert C_{AB} stets größer sein muß als der zuletzt gespeicherte Zählwert C_{AB}, können Replay-Attacken, d. h. Angriffe durch Wiedereinspielung abgehörter Daten, entdeckt werden.

Die erste Schlüsselaustauschnachricht SA1 wird von der zweiten Computereinheit C2 anhand des dritten Hash-Wertes $h(k, P, C_{AB}, I_B, AR_B)$ verifiziert, der Sitzungsschlüssel k wird unter Verwendung des geheimen Schlüssels SK_B der zweiten Computereinheit C2 entschlüsselt, und es wird eine zweite Schlüsselaustauschnachricht SA2 gebildet, mit der der Empfang und

die weitere Verwendung des Sitzungschlüssels k für die Verbindung P der ersten Computereinheit C1 bestätigt wird.

Die zweite Schlüsselaustauschnachricht SA2 enthält beispielsweise folgende Komponenten:

- die Verbindung P,
- einen vierten Hash-Wert $h(P, k, C_A, I_A)$, der gebildet wird mindestens über die Verbindung P, den Sitzungsschlüssel k, den ersten Zählwert C_A, sowie die Identitätsangabe I_A der ersten Computereinheit C1.

Auf diese Weise ist es möglich, auf einfache Art schnell und verläßlich in dem Verfahren zu verwendende Sitzungsschlüssel zwischen der ersten Computereinheit C1 und der zweiten Computereinheit C2 auszutauschen, ohne die gegenseitige Authentifikationsphase und die Aushandlung der Sicherheitspolitik SP wiederholen zu müssen.

Dies ist nur augrund des modularen Aufbaus des oben beschriebenen Verfahrens möglich, da bei dem modularen Aufbau einzelne Phasen des Verfahrens weggelassen oder in beliebiger Weise miteinander kombiniert werden können.

Ferner ist es in einer Weiterbildung vorgesehen, einen Verbindungsabbruch auch auf eine kryptographische Weise abzusichern. Dies kann beispielsweise dadurch erfolgen, daß von der ersten Computereinheit C1 eine Verbindungsabbruchsnachricht VAN gebildet wird und an die zweite Computereinheit C2 gesendet wird.

Die Verbindungsabbruchsnachricht VAN enthält beispielsweise folgende Komponenten:

- die Verbindung P,
- eine Angabe zur Identifizierung der Verbindungsabbruchsnachricht VAN,
- den Zählwert C_{AB},
- einen fünften Hash-Wert $h(P, DR, C_{AB}, I_B, AR_B)$, der bei-

spielsweise über die Verbindung P, die Angabe DR der Verbindungsabbruchsnachricht VAN, den Zählwert C_{AB}, die Identitätsangabe I_B der zweiten Computereinheit C2, und die Authentifikationsreferenz AR_B der zweiten Computereinheit C2 gebildet wird.

Die Verbindungsabbruchsnachricht VAN wird von der zweiten Computereinheit C2 verifiziert, die Verbindung wird abgebrochen, und es wird eine beispielsweise Verbindungsabbruchbestätigungsnachricht VACKN in der zweiten Computereinheit C2 gebildet und an die erste Computereinheit C1 übertragen.

Die Verbindungsabbruchbestätigungsnachricht VACKN enthält beispielsweise folgende Komponenten:

- die Verbindung P,
- eine Angabe DA zur Identifizierung der Verbindungsabbruchbestätigungsnachricht VACKN,
- einen sechsten Hash-Wert $h(P, DA, C_{AB}, I_A, AR_A)$, der beispielsweise über die Verbindung P, die Angabe DA zur Identifizierung der Verbindungsabbruchbestätigungsnachricht VACKN, den Zählwert C_{AB}, die Identitätsangabe I_A der ersten Computereinheit C1, sowie die Authentifikationsreferenz AR_A der ersten Computereinheit C1 gebildet wird.

Mit den Angaben DR, DA zur Identifizierung der Verbindungsabbruchsnachricht VAN bzw. der Verbindungsabbruchbestätigungsnachricht VACKN ist es möglich, Mißbrauch der Hash-Werte bei zukünftigen Erweiterungen dieser oben beschriebenen Verfahren für andere Zwecke zu verhindern. Die Verbindungsabbruchsnachricht VAN und/oder die Verbindungsabbruchbestätigungsnachricht VACKN enthalten zusätzlich die Angabe über die verwendete Verbindung P.

Die oben beschriebenen und in Fig. 1 dargestellten Phasen des Verfahrens zur Authentifizierung A, zur Aushandlung SP der Sicherheitspolitikvorschlag, zum Schlüsselaustausch SA, sowie

zum Verbindungsabbruch können in beliebiger Kombination miteinander durchgeführt werden.

Es ist in einer Weiterbildung des Verfahrens vorgesehen, daß in der Verbindungsabbruchphase nicht alle geheimen ausgetauschten Informationen sofort gelöscht werden, sondern daß zuerst nur der jeweils ausgetauschte Sitzungsschlüssel k gelöscht wird und beispielsweise die ausgehandelte Sicherheitspolitik und/oder die Authentifikationsreferenzen AR_A, AR_B in den Computereinheiten C1, C2 gespeichert bleiben.

Ferner ist es in einer Weiterbildung vorgesehen, die Löschung der geteilten geheimen Informationen sukzessive zu löschen, d. h. nach Löschen des Sitzungsschlüssels k zuerst die jeweils ausgehandelte Sicherheitspolitik zu löschen und erst anschließend die Authentifikationsreferenzen AR_A, AR_B.

Das Verfahren kann während einer Verbindungsaufbauphase bzw. während einer Verbindungsaufbauphase einer Verbindung zwischen der ersten Computereinheit C1 und der zweiten Computereinheit C2 durchgeführt werden.

In einer Weiterbildung des Verfahrens ist es vorgesehen, die einzelnen Nachrichten in einem Nachrichtenformat zu übertragen, dessen Aufbau in Figur 2 dargestellt ist.

Bei diesem Nachrichtenformat wird den jeweils zu übertragenden Nachrichten ein Kopffeld KF vorangestellt.

Das im weiteren beschriebene Nachrichtenformat ist in keinster Weise auf das im vorigen beschriebene Verfahren beschränkt, sondern kann in allen kryptographischen Protokollen verwendet werden.

Das Kopffeld KF weist vorzugsweise folgende Elemente auf:

- ein Sicherheits-Flag SF (Security-Flag) der Länge mindestens eines Bits,

- die Verbindung P,
- eine Phasenangabe PT einer Phase A, SP, SA, auf die sich die jeweilige Information der Nachricht bezieht,
- ein Zählerfeld Z, mit dem die Nachricht jeweils innerhalb der jeweiligen Phase A, SP, SA eindeutig identifiziert wird,
- eine Angabe D, beispielsweise eine Adresse, der die Nachricht empfangenden Computereinheit C1, C2 und/oder einer Angabe der Sicherheitsdomäne S1, S2, der die jeweilige Computereinheit C1, C2 zugeordnet ist.

Weiterhin können in dem Kopffeld KF in einer Weiterbildung auch beispielsweise in dem Feld PT, in dem die jeweilige Phase A, SP, SA angegeben wird, zusätzlich mindestens eine Angabe über in der Phase A, SP, SA zu verwendende Algorithmen, beispielsweise RSA, MD5, MD4, DES, Elliptische Kurve-Algorithmen und/oder in den Algorithmen zu verwendende Parameter enthalten sein.

Durch das Sicherheits-Flag SF, welches die Länge mindestens eines Bits aufweist, wird es für den Empfänger bei der Auswertung des Kopffeldes KF auf sehr einfache, schnelle und somit Rechenkapazität einsparende Weise möglich, zu erkennen, ob die jeweils empfangene Nachricht in irgendeiner Weise kryptographisch behandelt ist.

Hierzu reicht die Angabe in dem Sicherheits-Flag SF mit einem ersten logischen Wert für eine kryptographisch bearbeitete Nachricht und einen zweiten logischen Wert für eine kryptographisch nicht bearbeitete Nachricht aus.

Aus diesem Grund ist es in einer Weiterbildung vorgesehen, daß das Sicherheits-Flag SF nur die Länge genau eines Bits aufweist.

Ein Vorteil des Zählerfeldes Z ist darin zu sehen, daß in einer Phase A, SP, SA prinzipiell beliebig viele Nachrichten

ausgetauscht werden können und die jeweilige Nachricht innerhalb der Phase A, SP, SA mittels des Zählerfeldes Z eindeutig identifiziert werden kann.

Ein Vorteil der Phasenangabe PT der Phase A, SP, SA in dem Kopffeld KF ist in der sehr einfachen Erweiterbarkeit des gesamten Verfahrens um neue Phasen zu sehen, wobei lediglich eine neue Kennzeichnung in die Phasenangabe PT aufgenommen werden muß. Auch ist es mit der Phasenangabe PT ebenso einfach möglich, schon vorgesehene Phasen zu ersetzen und/oder zu löschen.

Die Nachricht selbst ist in einem Feld VL variabler Länge enthalten.

In diesem Dokument wurden folgende Veröffentlichungen zitiert:

[1] MMC-Übersichtsartikel

[2] S. Muftic, Sicherheitsmechanismen für Rechnernetze, Carl Hanser Verlag, München, ISBN 3-446-16272-0, S. 34 - 70, 1992

[3] E. Kipp et al, The SSL Protocol, Internet Draft, Erhältlich im Juni 1995 im Internet unter folgender Adresse:
gopher://ds.internic.net:70/00/internet-drafts/draft-hickman-netscape-ssl-01.txt

Patentansprüche

1. Verfahren zum kryptographischen Schlüsselmanagement zwischen einer ersten Computereinheit (C1) und einer zweiten Computereinheit (C2),
- bei dem zwischen der ersten Computereinheit (C1) und der zweiten Computereinheit (C2) eine Authentifikation durchgeführt wird,
- bei dem während der Authentifikation zwischen der ersten Computereinheit (C1) und der zweiten Computereinheit (C2) Authentifikationsreferenzen (AR_A, AR_B) ausgetauscht werden, mit denen die Authentizität der Computereinheiten (C1, C2) gewährleistet wird,
- bei dem zwischen der ersten Computereinheit (C1) und der zweiten Computereinheit (C2) eine Sicherheitspolitik (SP) ausgehandelt wird und/oder ein Schlüsselaustausch (SA) durchgeführt wird, und
- bei dem bei der Aushandlung der Sicherheitspolitik (SP) und/oder bei dem Schlüsselaustausch (SA) mindestens eine der Authentifikationsreferenzen (AR_A, AR_B) verwendet wird.

2. Verfahren nach Anspruch 1,
- bei dem die erste Computereinheit (C1) einer ersten Sicherheitsdomäne (S1) zugeordnet ist,
- bei dem die zweite Computereinheit (C2) einer zweiten Sicherheitsdomäne (S2) zugeordnet ist,
- bei dem von weiteren Computereinheiten (Ci) der ersten Sicherheitsdomäne (S1) oder der zweiten Sicherheitsdomäne (S2) eine weitere Sicherheitspolitik (SPi) ausgehandelt wird, und
- bei dem bei der Aushandlung die Authentifikationsreferenzen (AR_A, AR_B) verwendet werden.

3. Verfahren nach Anspruch 1 oder 2,
- bei dem die erste Computereinheit (C1) einer ersten Sicherheitsdomäne (S1) zugeordnet ist,
- bei dem die zweite Computereinheit (C2) einer zweiten Sicherheitsdomäne (S2) zugeordnet ist,

- bei dem von weiteren Computereinheiten (Ci) der ersten Sicherheitsdomäne (S1) oder der zweiten Sicherheitsdomäne (S2) ein weiterer Schlüsselaustausch (SAi) durchgeführt wird, und
- bei dem bei dem Schlüsselaustausch (SAi) die Authentifikationsreferenzen (AR_A, AR_B) verwendet werden.

4. Verfahren nach einem der Ansprüche 1 bis 3, bei dem im Rahmen des Verfahrens Hash-Funktionen (h()) verwendet werden, die auf symmetrischen Kryptoalgorithmen basieren.

5. Verfahren nach einem der Ansprüche 1 bis 4, bei dem im Rahmen des Verfahren Digitale Signaturen (SIG()) verwendet werden.

6. Verfahren nach einem der Ansprüche 1 bis 5, bei dem die Authentifikation nach einem Verfahren gemäß der starken Authentifikation des X.509-Verfahrens durchgeführt wird.

7. Verfahren nach einem der Ansprüche 1 bis 6,
- bei dem die Authentifikation nach einem Verfahren gemäß dem Diffie-Hellman-Verfahren zum Schlüsselaustausch durchgeführt, und
- bei dem die nach dem Diffie-Hellman-Verfahren ausgetauschten Schlüssel als Authentifikationsreferenzen (AR_A, AR_B) verwendet werden.

8. Verfahren nach einem der Ansprüche 1 bis 7, bei dem eine Verbindungsabbauphase (Disconnect) durchgeführt wird, in deren Rahmen geteilte Geheimnisse, beispielsweise der ausgetauschte Schlüssel oder die Authentifikationreferenzen (AR_A, AR_B) gelöscht werden.

9. Verfahren nach Anspruch 8, bei dem der ausgetauschte Schlüssel gelöscht wird.

10. Verfahren nach Anspruch 9,
bei dem anschließend sukzessive weitere Geheimnisse gelöscht werden.

FIG 1

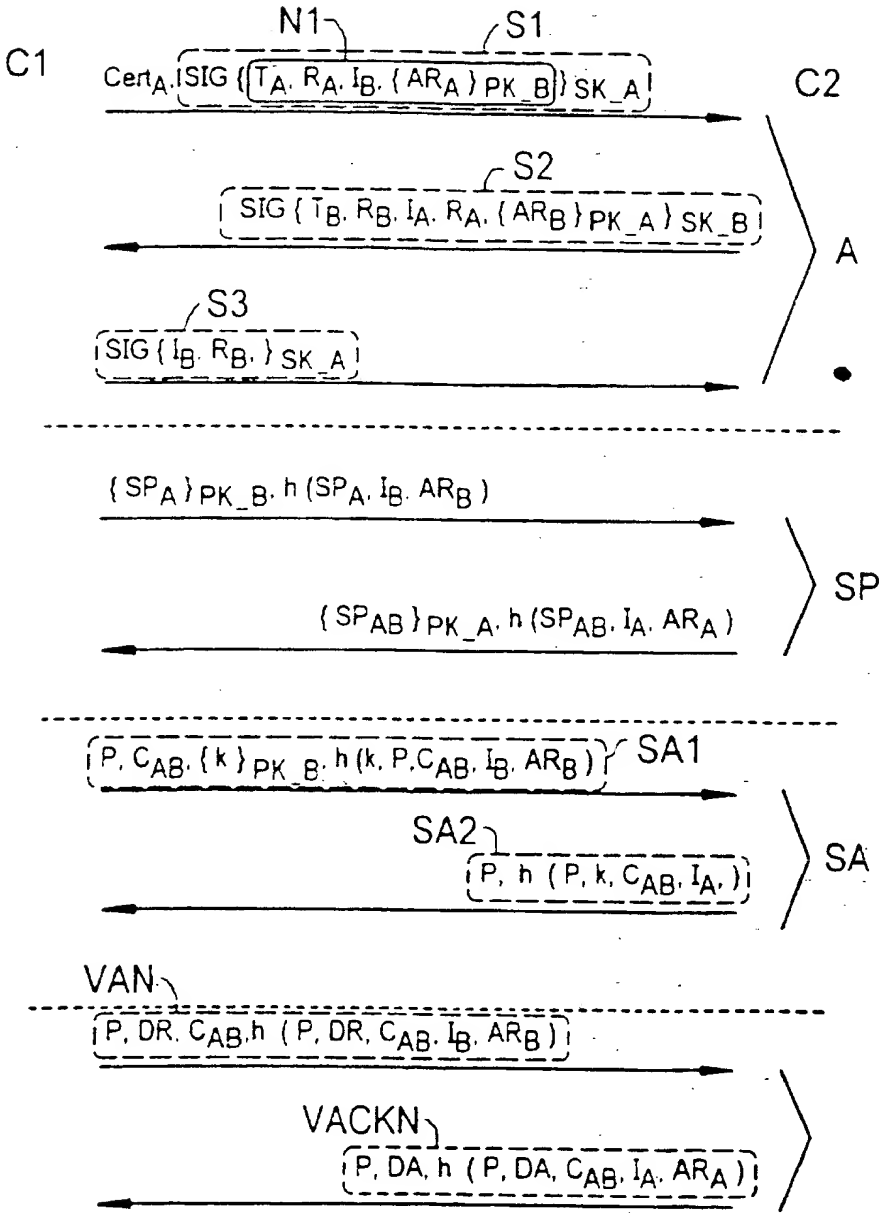
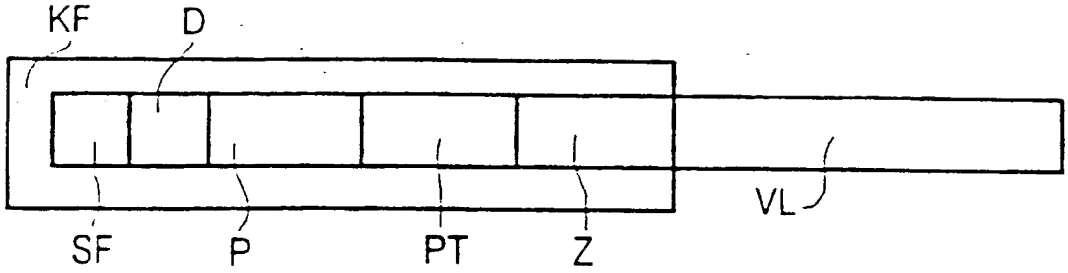


FIG 2



INTERNATIONAL SEARCH REPORT

Internat Application No
PCT/DE 97/01002

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 39 15 262 A (ASEA BROWN BOVERI) 30 November 1989	1,7
Y	see page 2, line 27 - page 3, line 4 see page 4, line 8 - last line --- -/--	1,2

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 October 1997	28. 10. 97

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CHORLEY B J ET AL: "The definition and implementation of a secure communications protocol" PROCEEDINGS OF THE INTERNATIONAL CARNAHAN CONFERENCE ON SECURITY TECHNOLOGY, ZURICH, SWITZERLAND, 4-6 OCT. 1983, ISBN 0-89779-057-X, 1983, LEXINGTON, KY, USA, UNIV. KENTUCKY, USA, pages 95-102, XP002043057 see page 96, left-hand column, line 23 - line 43 see page 96, right-hand column, paragraph 4 see page 96, right-hand column, last paragraph - page 97, left-hand column, line 21	1,2
A	see page 99, right-hand column	4,5

A	EP 0 602 335 A (MOTOROLA) 22 June 1994 see page 5, line 22 - page 6, line 11	1,2

A	US 5 224 163 A (GASSER AT AL.) 29 June 1993 see column 3, line 26 - line 43 see column 15, line 66 - column 16, line 5	8,9

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Internat' Application No
PCT/DE 97/01002

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 3915262 A	30-11-89	NONE	
EP 602335 A	22-06-94	US 5341426 A	23-08-94
		JP 6232861 A	19-08-94
		NO 933403 A	16-06-94
US 5224163 A	29-06-93	NONE	

INTERNATIONALER RECHERCHENBERICHT

Interne Aktenzeichen
PCT/DE 97/01002

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 H04L9/08

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	DE 39 15 262 A (ASEA BROWN BOVERI) 30.November 1989	1,7
Y	siehe Seite 2, Zeile 27 - Seite 3, Zeile 4 siehe Seite 4, Zeile 8 - letzte Zeile --- -/--	1,2

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
9.Oktober 1997	28. 10. 97

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	CHORLEY B J ET AL: "The definition and implementation of a secure communications protocol" PROCEEDINGS OF THE INTERNATIONAL CARNAHAN CONFERENCE ON SECURITY TECHNOLOGY, ZURICH, SWITZERLAND, 4-6 OCT. 1983, ISBN 0-89779-057-X, 1983, LEXINGTON, KY, USA, UNIV. KENTUCKY, USA, Seiten 95-102, XP002043057 siehe Seite 96, linke Spalte, Zeile 23 - Zeile 43 siehe Seite 96, rechte Spalte, Absatz 4 siehe Seite 96, rechte Spalte, letzter Absatz - Seite 97, linke Spalte, Zeile 21	1,2
A	siehe Seite 99, rechte Spalte	4,5

A	EP 0 602 335 A (MOTOROLA) 22.Juni 1994 siehe Seite 5, Zeile 22 - Seite 6, Zeile 11	1,2

A	US 5 224 163 A (GASSER AT AL.) 29.Juni 1993 siehe Spalte 3, Zeile 26 - Zeile 43 siehe Spalte 15, Zeile 66 - Spalte 16, Zeile 5	8,9

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/DE 97/01002

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 3915262 A	30-11-89	KEINE	
EP 602335 A	22-06-94	US 5341426 A	23-08-94
		JP 6232861 A	19-08-94
		NO 933403 A	16-06-94
US 5224163 A	29-06-93	KEINE	